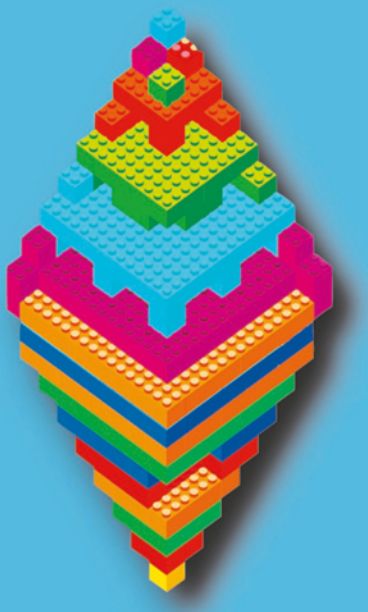
»Ich war noch nie so begeistert vom Potenzial des Internets, und das ist vor allem Vitalik Buterin zu verdanken«
ALEX OHANIAN, Reddit-Mitgründer, im TIME-Magazin

VITALIK BUTERIN



MEHR *als* GELD

Die Entstehung von Ethereum und die Zukunft von Blockchains

campus

Mehr als Geld

Vitalik Buterin, geb. 1994, ist ein russisch-kanadischer Programmierer und Autor, der 2011 das *Bitcoin Magazine* mitbegründete. 2014 schuf er mit Ethereum die Grundlage für die nach Bitcoin erfolgreichste Kryptowährung der Welt: Ether. 2021 wurde er vom *TIME Magazine* als eine der einflussreichsten Personen des Jahres ausgezeichnet.

Nathan Schneider ist Assistenzprofessor für Medienwissenschaft an der University of Colorado in Boulder und Autor von *Everything for Everyone: The Radical Tradition that Is Shaping the Next Economy*.

Vitalik Buterin

MEHR ALS GELD

Die Entstehung von Ethereum und die Zukunft von Blockchains

Herausgegeben von Nathan Schneider
Aus dem Englischen von Thorsten Schmidt

Campus Verlag
Frankfurt/New York

Die englische Originalausgabe erschien 2022 bei Seven Stories Press
unter dem Titel *Proof of Stake: The Making of Ethereum and the Philosophy of Blockchains*

ISBN 978-3-593-51679-0 Print
ISBN 978-3-593-45326-2 E-Book (PDF)
ISBN 978-3-593-45327-9 E-Book (EPUB)

Redaktion: Britta Fietzke
Umschlaggestaltung: Guido Klütsch, Köln nach einem Entwurf von Seven Stories Press
Satz und Innengestaltung: Oliver Schmitt, Mainz
Gesetzt aus der Minion und Avenir
Druck und Bindung: Beltz Grafische Betriebe, Bad Langensalza
Beltz Grafische Betriebe ist ein klimaneutrales Unternehmen (ID 15985-2104-1001).
Printed in Germany.

www.campus.de

INHALT

Für meine Mutter und meinen Vater,
tolle und liebevolle Eltern, Unternehmer
und Internet-Meme-Lords

EINLEITUNG

Von Nathan Schneider

Bevor er im Alter von 19 Jahren damit anfing, eine neue ökonomische Infrastruktur für das Internet aufzubauen, bevor er zum Milliardär wurde, der auf der Couch von Freund:innen schläft, wollte Vitalik Buterin bereits eins: schreiben. Er interessierte sich auf Anregung seines Vaters hin, mit dem er als Kind von Russland nach Kanada ausgewandert war, für Bitcoin. Er hat seine ersten Coins aber nicht etwa gekauft, geliehen oder geschürft, vielmehr fragte er 2011 in einem Onlineforum, ob ihn wohl jemand mit Bitcoin bezahlen würde, wenn er darüber schriebe.

Jemand tat es. Und Buterin machte das Schreiben weiterhin Spaß, so sehr, dass er das *Bitcoin Magazine* mitbegründete, ein als Print und digital verfügbares Magazin, das die neuesten Entwicklungen einer damals noch äußerst kleinen und unbekannten Subkultur festhält. Dieses neue, nicht gerade benutzerfreundliche Internetgeld fesselte Buterins Aufmerksamkeit mehr als das College im ersten Jahr. Seit er sich einst selbst zum Reporter ernannte, entwickelte er seine Ideen in fortgesetztem Gespräch mit anderen. In den diversen Schriften, die er im Laufe der Jahre breit gestreut in Blogs, Foren sowie als Tweets veröffentlichte, trat immer deutlicher eine unverwechselbare Stimme hervor, und – zum Teil wegen dieser Stimme – hat er ein Publikum für sich gewonnen, das fast schon hingerissen alles verfolgt, was er über seine Erfindung, Ethereum, zu Papier bringt. Wenn Ethereum und seinesgleichen jedoch zu jener Art allgegenwärtiger Infrastruktur werden, wie sie es laut ihrer Erfinder sollen, müssen die Ideen

von einer breiteren Öffentlichkeit verstanden – und kritisch hinterfragt – werden.

Dieses Buch führt in die Schriften Vitalik Buterins ein.

Als die unter dem Pseudonym Satoshi Nakamoto firmierende Person 2008 – inmitten der Turbulenzen der Weltfinanzkrise – den Bitcoin-Prototyp ankündigte, wollte man eine Währung erschaffen, die von kryptografischen Computernetzwerken statt von Regierungen oder Banken verwaltet werden sollte. Sie wurde »Kryptowährung« genannt. Libertäre Goldhamster und Techie-Cypherpunks schwelgten in den Metaphern des Systems: digitales Mining (Schürfen), begrenztes Angebot, bargeldartige Transaktionen, die sicher und vertraulich sein konnten. Buterin hatte die gleichen Instinkte wie dieses frühe Zielpublikum. Im Zuge seiner immer näheren Beschäftigung mit Bitcoin erkannte er aber gegen Ende 2013 allmählich, dass die Bitcoin zugrunde liegende Blockchain-Technologie die Basis für etwas Größeres sein könnte: ein Tool, um im Internet heimische Organisationen, Unternehmen und ganze Wirtschaftssysteme zu erschaffen. Also schrieb er darüber. Das *Ethereum Whitepaper* – das Gründungsdokument, das Sie auf der Campus-Website herunterladen können – elektrisierte die noch immer kleine Welt der Kryptowährungen, als es gegen Ende des Jahres erschien. Statt von den gängigen Unternehmen, Investor:innen und Gesetzen, die die Server kontrollierten, abhängig zu sein, würde Ethereum standardmäßig von den Usern verwaltet. Anstatt den Bitcoin-Metaphern von Gold und Minen, folgte die Ethereum-Kultur der Ästhetik von Buterins Lieblings-T-Shirts, mit Robotern, Einhörnern und Regenbogen als bevorzugte Maskottchen.

Seit Ethereums Onlinegang 2015 wurden viele weitere, konkurrierende Blockchains entwickelt, die jeweils auf andere Weise Ähnliches leisten können. Ethereum bleibt jedoch die größte unter ihnen. Obgleich seine Währung, »Ether« (ETH) genannt, im Vergleich zu Bitcoin bezüglich ihrer Gesamtkapitalisierung nur abgeschlagen auf dem zweiten Platz landet, hat Ethereum, wenn man den Wert sämtlicher Produkte und Community-Token, die aus der Basis von Ethereum entwickelt wurden, zusammennimmt, den größten Anteil an diesem fremdartigen neuen Wirtschaftssystem. Während der ersten Testläufe des Projekts wurde Buterin immer mehr zum »wohlwollenden Diktator« Ethereums – ob es ihm nun gefiel oder

nicht –, nicht kraft einer offiziell bekleideten Position, sondern aufgrund des von ihm eingeflößten Vertrauens. Die hier versammelten Schriften sind von zentraler Bedeutung für den Aufbau dieses Vertrauens gewesen.

Hierbei ist Buterins eigene Position von Widersprüchen geprägt. Einerseits zeigt er völlig neue Wege für die Selbstorganisation von Menschen auf, andererseits enthält er sich jeglicher Meinungsäußerung bezüglich der Nutzung dieser Macht durch Menschen. Wie einer der nachstehenden Aufsätze erläutert, ist »glaubwürdige Neutralität« ein Grundsatz des Systemdesigns, aber auch eine Beschreibung der Rolle, die er als eine Führungsperson mittlerweile einnimmt – von den frühesten Personalentscheidungen für die *Ethereum Foundation* bis zu den jüngsten risikoreichen Software-Updates. Obwohl er alles in seiner Macht Stehende dagegen unternahm, ließ sich seine führende Rolle kaum von Ethereum selbst trennen. Während Ethereum und vergleichbare Systeme auf der Annahme basieren, dass Menschen egoistisch seien, ist er der Asketiker, der – abgesehen von dem Wunsch, einer zukünftigen Krypto-Welt den Weg zu ebnen – für sich selbst nichts Besonderes zu wollen scheint.

Es gibt jedoch keine Garantien dafür, dass dies eine wünschenswerte Zukunft ist. Als Buterin auf einer Bitcoin-Konferenz in Miami Anfang 2014 Ethereum erstmals auf der Bühne vorstellte, beendete er seinen Vortrag, nach einer langen Auflistung all der wunderbaren Sachen, die sich damit verwirklichen ließen, mit einem Paukenschlag: der Erwähnung von Skynet, die künstliche Intelligenz in den *Terminator*-Filmen, die sich gegen ihre menschlichen Erfinder wendet. Es war ein Scherz, den er später wiederholen sollte, aber wie so viele abgedroschene Scherze enthielt er auch eine Warnung. Ethereum birgt in sich das Potenzial sowohl zu einer utopischen als auch einer dystopischen Gesellschaft – sowie auch für alles dazwischen:

- Es erzeugt eine künstliche Knappheit, indem es die Verfügbarkeit hergestellter Token begrenzt; aber diese ermöglichen Communitys die Generierung großer Mengen an gezielt einsetzbarem und kontrollierbarem Kapital.
- Es schließt Menschen aus, die riskantes Internetgeld nicht kaufen und nicht handeln können oder wollen; es beflügelte auch die Erfindung

neuartiger Governance-Systeme, die mit nie dagewesener Inklusion die Macht aufteilen.

- Über viele Jahre hinweg verbrauchte es riesige Mengen an Energie nur für die Aufrechterhaltung des Betriebs; zugleich ermöglicht es eine neue Art der Bepreisung von Kohlenstoff und umweltverschmutzenden Aktivitäten, während sich Regierungen diesem Aspekt weiterhin verweigern.
- Es hat Neureiche hervorgebracht, die dafür verrufen sind, einen verschwenderischen Lebensstil zu führen, sich in Steueroasen zu versammeln und bereit zu sein, so hohe Preise zu zahlen, dass die Einheimischen verdrängt werden. Es ist auch ein grenzenloses Finanzsystem im Besitz seiner User, das für jeden mit Smartphone in der Hand zugänglich ist.
- Es belohnt eine technikaffine Elite von Early Adopters; zugleich bietet es eine echte Chance, die dominanten Technologiekonzerne zu untergraben.
- Es hat ein spekulatives Finanzsystem geschaffen, bevor es eine Realwirtschaft nützlicher Produkte hervorgebracht hat; aber viel mehr als auf einem Aktienmarkt liegt das Eigentum bei den Wert schaffenden Menschen.
- Es hat den Besitzer:innen digitaler Sammlerobjekte von augenscheinlich nur geringem Wert enorme Gewinne beschert; in der Folge entstand ein neues Geschäftsmodell, das den Aufbau und das Sharing innerhalb einer Open-Access-Kultur unterstützt.
- Es verspricht, frühzeitige User auf Kosten zukünftiger Generationen reich zu machen; es gibt diesen Generationen eine Reihe von Bausteinen an die Hand, die diese als Bauende völlig frei verwenden können.

Die Leser der folgenden Aufsätze müssen sich dieser Widersprüche bewusst sein und sich mit ihnen auseinandersetzen, um für sich selbst und ihre Communitys herauszufinden, welche Optionen sich durchsetzen sollten. Die Widersprüche können ärgerlich, aber auch motivierend sein. Sie sind noch frisch genug, um sich formen zu lassen.

Im Zentrum jedes Systems auf Blockchain-Basis wie Bitcoin oder Ethereum steht der Konsens, einem Prozess, mithilfe dessen sich Rechner auf einen gemeinsamen Datensatz einigen und diesen vor Manipulation schüt-

zen – unabhängig davon, ob es sich dabei um eine Liste von Transaktionen, wie bei Bitcoin, oder den Zustand des Ethereum-Weltrechners handelt. Die Erreichung eines Konsenses ist ohne eine zentrale Autorität keine leichte Angelegenheit. Bitcoin nutzt einen als »Arbeitsnachweis« (»Proof of Work«) bezeichneten Ansatz, was bedeutet, dass viele Computer eine Menge Energie für die Lösung mathematischer Aufgaben aufwenden, mit denen wiederum der Nachweis erbracht wird, dass sie sich ernsthaft um die Sicherheit des Systems bemühen. Die Menschen hinter diesen Rechnern, die sogenannten »Miner« (Schürfer:innen), werden dafür bezahlt und haben dabei ungefähr den gleichen Elektrizitätsverbrauch wie ein ganzes Land, wobei sie auch dem Verbrauchsniveau entsprechende Kohlenstoffemissionen erzeugen. In Ermangelung einer passenden Alternative übernahm Ethereum ebenfalls das Proof-of-Work-Verfahren, aber schon vor der Onlineschaltung sprach Buterin über die Umstellung auf einen anderen Mechanismus, die erfolgen sollte, sobald sein Team die damit verbundenen Probleme gelöst hätte: den »Proof of Stake« (»Anteils- oder Einsatznachweis«). Beim Proof of Stake beweisen User mithilfe von Token-Guthaben statt von Rechenleistung ihr berechtigtes Interesse am Prozess. Der Energieverbrauch ist minimal. Wenn Token-Besitzer:innen das System zu korrumpieren versuchen, verlieren sie die »gestaketen« Token. Im September 2022 hat Ethereum schließlich den Umstieg auf Proof of Stake abgeschlossen.

Konsensmechanismen sind hier sowohl Metaphern als auch Systemdesigns, denn sie sind eine Erinnerung an die in diesen Essays beschriebene geleistete Arbeit, den Einsatz, den Glauben dahinter und die Koordination des Ganzen. Sie verdeutlichen auch die Widersprüche: Innovation und Verschwendung, Demokratie und Plutokratie, pulsierende Gemeinschaft und unablässiges Misstrauen. Diese Metaphern widersetzen sich wie die Mechanismen selbst der idealistischen Überhöhung und verweisen auf die notwendigen Kompromisse, um auch nur Teile einer erhofften Welt in der realen Welt überleben zu lassen.

Die Aufsätze in diesem Buch, die zusammen mit Buterin ausgewählt wurden, zeigen eine besondere Seite von ihm: den Gesellschaftstheoretiker und Aktivisten, eine Person, die ihr Handeln reflektiert und die sich dabei der Konsequenzen bewusst wird. Das weitgehend junge, männliche und

privilegierte Milieu der Krypto-Kultur scheint oftmals jener Probleme, die ihre User vorgeblich lösen wollen, selbst ganz enthoben zu sein. In Buterin spiegelt sich diese Kultur wider: Mitunter schreibt er recht technisch, hier aber weniger als in anderen Schriften, von denen sich viele ausschließlich an andere Entwickler:innen richteten. Die technischen Teile belohnen die Mühen, die man für ein Verständnis auf sich nehmen muss; selbst bei Formeln bemüht er sich um eine klare, verständliche und auch witzige Darstellung.

Die Aufsätze wurden im Interesse stilistischer Einheitlichkeit leicht redigiert. Verweise auf Hyperlinks, die in einem gedruckten Buch nicht direkt aufgerufen werden können, wurden entfernt. Da sie ursprünglich für das Publikum einer gemeinsamen Subkultur geschrieben wurden, enthalten die Aufsätze gelegentlich nachträglich eingefügte Anmerkungen zu Anspielungen, die vielleicht außerhalb der Krypto-Sphäre nicht direkt verständlich sind.

Jetzt, da Krypto sich langsam einen Weg in das gewöhnliche Wirtschaftsleben bahnt, wird immer heftiger darüber diskutiert, ob dieser Geist wieder in die Flasche gesperrt werden sollte – sofern dies noch möglich ist. Die Lektüre dieses Buches könnte diejenigen, die sich zunächst über das *Ob* den Kopf zerbrachen, dazu bringen, sich den stetig wachsenden Fragen um das *Wie* zuzuwenden. Wenn dies wirklich der Anfang einer neuen sozialen Infrastruktur ist, werden die politischen und kulturellen Gewohnheiten, die wir heute in Bezug auf die Krypto-Technologie entwickeln, später weitreichende Folgen haben. Buterins Betrachtungen verdeutlichen, dass das *Wie* noch eine weitgehend offene Frage bleibt.

TEIL 1
PRE-MINING

Buterin berichtet in einem Blog-Eintrag im Januar 2014, er habe das *Ethereum Whitepaper* »an einem kalten Novembertag in San Francisco geschrieben, als krönenden Abschluss monatelangen Nachdenkens und oftmals frustrierender Arbeit«.[1] In jenen Monaten war er halb Chronist (für das *Bitcoin Magazine*) und halb Erbauer (er packte bei mehreren Bitcoin-Start-ups mit an); er besuchte Libertäre in New Hampshire, Expats in Zürich, Codierer in Tel Aviv und die Bewohner:innen Calafous, einer »postkapitalistischen Kolonie« in einem verfallenden Fabrikkomplex nahe Barcelona. Bitcoin wurde erstmals in einem Whitepaper angekündigt und es wurden seither andere Krypto-Projekte in der gleichen Form öffentlich vorgestellt: Stelle noch vor dem Software-Release ein Dokument öffentlich, das zugleich Manifest und technische Spezifikation ist. Dieses Genre passte gut zu Buterins eigenem Werdegang als Schriftsteller und Erfinder im Jahr 2013. »Ethereum: Eine Kryptowährung der nächsten Generation und eine dezentrale Anwendungsplattform« ist eine hervorragende Zusammenfassung des vollständigen Whitepapers. Schon anderthalb Jahre vor der Erstveröffentlichung von Ethereum macht er sich Gedanken über Ethereum 2.0 und das Proof-of-Stake-Verfahren, das erst im Jahr 2022 eingeführt werden sollte.

»Pre-Mining« bezeichnet den Prozess der Token-Schöpfung vor der Veröffentlichung einer Blockchain. Durch den Verkauf von »vorgeschürfter (also vor der Markteinführung)« (»premined«) ETH auf der Basis des *Ethereum Whitepapers* nahmen Buterin und seine frühen Mitstreiter Bitcoin im Wert von über 18 Millionen Dollar ein. Damit stellten sie einen Rekord als das bis dato größte Online-Crowdfunding auf – der seitdem vor allem von Crowdfunding-Projekten auf Ethereum selbst überboten wurde. Trotz des Drucks seitens älterer, erfahrener Projektmitarbeiter, die ein kommerzielles Unternehmen gründen wollten, bestand Buterin darauf, Ethereum über eine gemeinnützige Stiftung aufzubauen. Das geschah jedoch nicht aus reiner Wohltätigkeit heraus, denn er und seine Mitgründer könnten mit ihren premined Token bei einem Erfolg erkleckliche Gewinne einfahren.

Diese Aufsätze zeichnen Buterins Wandlung von einem cyberlibertären »Widerstandskämpfer« zu einem pragmatischen, ein breites Spektrum abdeckenden Infrastruktur-Erbauer nach. Zuerst jubelte er damals aufkommenden Bitcoin-bezogenen Projekten zu, von denen nur sehr wenige überlebt haben. Der spätere, nachdenklichere Essay *Über Silos* zeigt, dass Buterin keine Antworten von einem einzelnen Projekt erwartet. Um Menschen zu befähigen, ihre Gesellschaftsverträge von Grund auf umzuschreiben, so Buterin, bedürfe es eines Instrumentariums ohne bestimmte Ideologie.

Im Vorfeld der Ethereum-Veröffentlichung fragt sich Buterin selbst: »Wozu ist es letzten Endes überhaupt von Nutzen?« Er skizzierte eine Theorie des Wandels, die weniger auf großartigen Disruptionen als auf der Lösung eher randständiger Probleme beruht. Die Überzeugungen, die die Entwickler:innen dieser Technologie motivierten, so sagt er voraus, würden sich in dem zeigen, was wiederum andere damit erschaffen würden. Während er sich auf die öffentliche Einführung vorbereitet, drehen sich seine Überlegungen zunehmend um das, was niemand wissen oder kontrollieren könne.

– N. S.

MÄRKTE, INSTITUTIONEN UND WÄHRUNGEN: EINE NEUE METHODE DER SOZIALEN INCENTIVIERUNG

Bitcoin Magazine, 10. Januar 2014

Bisher gab es vor allem zwei Lösungskategorien für das Problem, Anreize für produktive Aktivitäten zu schaffen: Märkte und Institutionen. Märkte sind in ihrer reinen Form vollständig dezentralisiert; sie bestehen aus einer fast grenzenlosen Anzahl von Agenten, die jeweils miteinander in Zweierinteraktionen treten, die wiederum beide Parteien jeweils besserstellen. Institutionen andererseits sind ihrem Wesen nach hierarchisch (»top-down«) geordnet, sie haben eine Governance-Struktur, die bestimmt, was zu jedem beliebigen Zeitpunkt die nützlichsten Aktivitäten sind, und die Menschen eine Belohnung für die Ausführung zuweist. Zentralisierung erlaubt es einer Institution, Anreize für die Produktion öffentlicher Güter zu schaffen, von denen Tausende oder sogar Millionen von Menschen profitieren, auch wenn der Nutzen für jede einzelne Person außerordentlich gering sein mag. Andererseits bringt Zentralisierung, wie wir alle wissen, wiederum eigene Risiken mit sich. In den letzten 10 000 Jahren waren diese beiden Optionen im Wesentlichen die einzige Auswahl. Mit dem Aufkommen von Bitcoin und seiner Abkömmlinge könnte sich dies jedoch schon bald ändern, und vielleicht erleben wir gerade den Beginn einer dritten Form der Incentivierung: Währungen.

Die Kehrseite der Medaille

Üblicherweise werden einer Währung drei grundlegende gesellschaftliche Funktionen zugeschrieben: Sie dient einerseits als Tauschmittel, das es Menschen erlaubt, Güter gegen Geld zu (ver-)kaufen, sodass man nicht dazu gezwungen wird, jemanden zu finden, der zur selben Zeit das hat, was man selbst haben will, und der oder die genau das braucht, was man selbst hat, um mit dieser Person dann ein Tauschgeschäft einzugehen. Geld dient außerdem als Wertspeicher, sodass wir zu unterschiedlichen Zeitpunkten produzieren und konsumieren können, und als Rechnungseinheit oder Maßstab, mit dem wir eine konstante »Produktmenge« messen können. Viele Menschen wissen jedoch nicht, dass Geld noch eine vierte Rolle spielt, deren Bedeutung im Verlauf der Geschichte größtenteils verheimlicht wurde: Seigniorage.

Seigniorage, der Geldschöpfungsgewinn, lässt sich formal definieren als die Differenz zwischen dem Marktwert einer Währung und ihrem intrinsischen (Material-)Wert – das heißt dem Wert, den sie hätte, wenn niemand sie als Währung benutzen würde. Bei sehr alten Währungen wie Getreide war die Seigniorage im Wesentlich gleich null, aber mit zunehmender Komplexität von Wirtschaftssystemen und Währungen sollte dieser von Geld scheinbar aus dem Nichts erschaffene »Phantomwert« immer mehr gesteigert werden. Schließlich erreichte er den Punkt, an dem die Seigniorage (wie im Fall moderner Währungen wie dem Dollar und Bitcoin) den gesamten Wert der Währung ausmacht.

Aber was geschieht mit der Seigniorage? Im Fall von Währungen, die auf natürlichen Ressourcen wie etwa Gold basieren, geht ein Großteil des Wertes einfach verloren. Jedes einzelne Gramm Gold entsteht durch die Arbeit eines Bergarbeiters, der es gewinnt; zunächst machen einige Goldgräber einen Gewinn, aber auf einem effizienten Markt sind alle leichten Gelegenheiten (für lukrative Geschäfte) bald erschöpft, und die Produktionskosten nähern sich dem Ertrag. Natürlich gibt es intelligente Methoden, um trotzdem aus Gold eine Seigniorage herauszuholen; in antiken Gesellschaften zum Beispiel prägten Könige Goldmünzen, die mehr wert

waren als gewöhnliches Gold, weil die Münzen das unausgesprochene Versprechen seitens des Königs beinhalteten, dass sie nicht gefälscht waren. Im Allgemeinen aber floss der Wert niemand Bestimmtem zu. Beim US-Dollar sahen wir eine geringfügige Verbesserung: Ein Teil der Seigniorage floss der US-Regierung zu. Dies war in vielerlei Hinsicht ein großer Schritt nach vorn, aber in anderer Hinsicht auch eine bis zuletzt unvollständige Revolution – nachdem Geld die Vorteile einer zentralisierten Seigniorage erlangt hatte, lastete es sich auch deren Risiken auf, indem es sich ins Herz einer der größten zentralisierten Institutionen der Menschheitsgeschichte einbettete.

Bitcoin betritt die Bühne

Vor fünf Jahren kam eine neue Art von Geld auf: Bitcoin. Wie beim Dollar besteht auch beim Bitcoin der Geldwert zu 100 Prozent aus Seigniorage, denn ein Bitcoin hat keinen Materialwert. Wohin aber fließt die Seigniorage? Ein Teil fließt den Minern (Schürfer:innen) als Gewinn zu, während der Rest die Schürfausgaben finanziert – Ausgaben für die Absicherung des Bitcoin-Netzwerks. In diesem Fall haben wir folglich eine Währung, deren Seigniorage direkt in die Finanzierung eines öffentlichen Gutes fließt: die Sicherheit des Bitcoin-Netzwerks selbst. Die Bedeutung dieses Aspekts wird massiv unterschätzt: Wir haben es hier mit einem dezentralisierten Prozess der Incentivierung zu tun – ohne Autorität oder Kontrolle –, der zugleich ein öffentliches Gut produziert, all dies aus dem ätherischen »Phantomwert«, der irgendwie von Menschen erzeugt wird, weil sie Bitcoin untereinander als Tausch- und Wertaufbewahrungsmittel nutzen.

Anschließend gab es die Einführung von Primecoin, der ersten Währung, die ihre Seigniorage für einen über sie selbst hinausgehenden Zweck nutzen wollte: Statt Miner letztlich nutzlose SHA256-»Hashes« berechnen zu lassen, verlangt Primecoin von den Minern, dass sie Cunningham-Ketten aus Primzahlen finden. Damit unterstützt die Kryptowährung eine enge Kategorie wissenschaftlicher Berechnungen und schafft zugleich einen Anreiz für Computerhersteller, herauszufinden, wie sich Schaltkreise besser für arithmetische Berechnungen optimieren lassen. Sie verzeichnete schnelle

Wertsteigerungen und steht auch heute noch auf der Beliebtheitsskala auf dem elften Rang – auch wenn ihr größter praktischer Nutzen für einzelne User – die »Block Time« von 60 Sekunden (durchschnittliche Zeit für das Schürfen eines neuen Blocks) – von vielen anderen, weitaus unbekannteren Währungen geteilt wird.

Ein paar Monate später, im Dezember, erlebten wir den Aufstieg einer Währung, die noch exzentrischer und deren Erfolg noch überraschender ist: Dogecoin. Dogecoin, mit dem Währungssymbol DOGE, ist eine Währung, die aus technischer Sicht fast völlig identisch zu Litecoin ist – lediglich wird die maximale Versorgung 100 Milliarden statt 84 Millionen Coins betragen. Schon jetzt aber hat die Währung eine maximale Marktkapitalisierung von 14 Millionen Dollar erreicht, was sie zur sechstgrößten der Welt macht, und *Business Insider* und *Vice* eine Erwähnung wert war. Was also ist so besonders an DOGE? Im Wesentlichen das Internet-Meme. »Doge«, ein Slang-Wort für »Dog«, das erstmals im Jahr 2005 in der *Homestar Runner*-Cartoon-Serie auftauchte, ist seither zu einem weltweiten Phänomen geworden, begleitet von der Praktik, Ausdrücke wie »wow«, »so style« und »such awesome« in bunter Comic-Sans-Schriftart über einen Shiba Inu im Bildhintergrund zu schreiben. Dieses Meme repräsentiert das gesamte Branding des Dogecoin; die Doge-Ikonografie prangt auf all seinen Community-Websites und Foren einschließlich der offiziellen Dogecoin-Website, des obligatorischen Launch-Threads auf Bitcointalk[2] und der Sub-

reddits /r/dogecoin und /r/dogecoinmarkets. Mehr bedurfte es nicht, um einen Litecoin-Klon auf einen Wert von 14 Millionen Dollar zu bringen.

Ein drittes Beispiel kommt schließlich von außerhalb des Kryptowährungsraums: Ven, eine eher traditionelle, zentralisierte Währung, die mit einem Korb voller Güter unterlegt ist, zu denen Rohstoffe, Währungen und »Futures« (Terminkontrakte) gehören. Vor Kurzem erweiterte Ven seinen Korb noch um Kohlenstoff-Futures, was es zur ersten Währung machte, die in gewisser Weise »mit der Umwelt verbunden« ist. Der Grund dafür ist ein kluger ökonomischer Hack, denn die Kohlenstoff-Futures unterlegen den Wert des Ven auf negative Weise, das heißt, der Währungswert steigt, wenn die Gesellschaft kohlendioxidärmer produziert und Kohlendioxidemissionszertifikate weniger lukrativ werden. Folglich hatten alle Ven-Besitzer:innen einen – wenn auch nur geringen – ökonomischen Anreiz, einen umweltfreundlichen Lebensstil zu unterstützen. Das Interesse der Menschen an Ven liegt zumindest teilweise an diesem Merkmal.

Insgesamt zeigen diese Beispiele, dass alternative Währungen in hohem Maße auf Graswurzel-Marketing angewiesen sind, damit sie auf breiter Front übernommen werden; niemand nimmt Bitcoin, Primecoin, Dogecoin oder Ven von Verkäufer:innen an, die Klingelputzen betreiben oder Händler:innen dazu überreden, sie zu akzeptieren, und nicht nur die technische Überlegenheit einer Währung entscheidet über ihre Popularität – Ideale spielen eine ebenso große Rolle. Es waren die Ideale Bitcoins, die WordPress, Mega und jetzt Overstock dazu bewogen, Bitcoin anzunehmen, und aus dem gleichen Grund dürfte wohl Ripple, ungeachtet seiner technischen Überlegenheit gegenüber Bitcoin für Händler:innen (insbesondere aufgrund seiner Bestätigungszeit von fünf Sekunden), als Zahlungsmethode bislang keine große Zugkraft entfaltet haben – seine Natur als ein halb-zentralisiertes Protokoll, hinter dem ein Unternehmen steht, das 100 Prozent der Geldversorgung an sich selbst ausgab, macht es unattraktiv für viele Kryptowährungsfans, denen an Fairness und Dezentralisierung liegt. Und heute sind es die Ideale Primecoins und Dogecoins – die Unterstützung der Wissenschaft einerseits beziehungsweise eine »Währung mit Spaß« andererseits –, die beide Währungen am Leben halten.

Aus diesen vier Beispielen lässt sich zusammen mit dieser Idee des Seigniorage-Phantomwertes ein mögliches Modell für eine neue Art »ökonomischer Demokratie« ableiten: Es ist möglich, Währungen aufzulegen, deren Seigniorage beziehungsweise Emission gewisse Anliegen unterstützt, und Menschen können für diese Anliegen stimmen, indem sie in ihren Firmen gewisse Währungen annehmen. Wenn man keine eigene Firma hat, kann man sich stattdessen an den Marketingbemühungen beteiligen und auf Unternehmen zur Annahme der Währung einwirken. Jemand könnte SocialCoin kreieren – eine Währung, die allen Menschen auf der Erde jeden Monat 1000 Einheiten schenkt, und wenn die Idee genügend Menschen gefällt und sie diese Währung annehmen, dann besteht plötzlich ein globales Dividendenprogramm für Bürger:innen ohne zentralisierte Finanzierung. Wir können auch Währungen mit Anreizen für die medizinische Forschung, die Erkundung des Weltalls oder künstlerische Betätigungen erschaffen; tatsächlich gibt es Künstler:innen, Podcaster:innen und Musiker:innen, die inzwischen darüber nachdenken, genau zu diesem Zweck ihre eigenen Währungen aufzulegen.

Im Fall eines besonderen öffentlichen Gutes, des »Computational Research« (wissenschaftliches Rechnen), können wir sogar noch weitergehen und den Distributionsprozess automatisieren. Computational Research kann durch einen Anreizmechanismus gefördert werden, der bislang in der realen Welt noch nicht in nennenswertem Umfang angewendet, jedoch vom Peercoin- und Primecoin-Erfinder Sunny King theoretisch begründet wurde: »Proof of Excellence« (sinngemäß »Vorzüglichkeitsnachweis«). Diesem Gedanken liegt folgende Idee zugrunde: Die Größe des Anteils einer Person an dem dezentralisierten Stimmrechtspool der Währung und ihre Belohnung richtet sich nicht nach ihrer Rechenleistung oder der Anzahl der bereits besessenen Münzen, sondern nach ihrer Fähigkeit, Lösungen für komplexe mathematische oder algorithmische Probleme zu finden, von denen die gesamte Menschheit profitieren würde. Wenn man zum Beispiel Forschungen auf dem Gebiet der Zahlentheorie durch Anreize fördern will,

kann man die »RSA Integer Factoring Challenges« in die Währung einbetten und festlegen, dass die Währung der ersten Person mit einer Lösung für das Problem automatisch 50 000 Einheiten plus gegebenenfalls das Recht, über gültige Blocks im Miningprozess abzustimmen, gewährt. Theoretisch könnte diese sogar zu einem Standardelement im Emissionsmodell jeder Währung werden.

Selbstverständlich ist die Idee, Währungen so zu nutzen, nicht neu – »soziale Währungen«, die auf kommunaler Ebene gelten, gibt es seit über 100 Jahren. In den letzten Jahrzehnten hat aber die Bewegung der sozialen Währungen gegenüber ihrem Höhepunkt zu Beginn des 20. Jahrhunderts etwas an Bedeutung verloren, hauptsächlich weil soziale Währungen immer nur eine äußerst begrenzte lokale Reichweite hatten und weil sie nicht von den Effizienzen des Bankensystems profitierten, die etablierteren Währungen wie dem US-Dollar zugutekamen. Bei Kryptowährungen fallen diese Einwände jedoch nun weg – sie sind ihrem Wesen nach global und profitieren von einem unglaublich leistungsfähigen digitalen Bankensystem, das direkt in ihren Quellcode eingebrannt ist. Daher könnte jetzt der perfekte Zeitpunkt für ein kraftvolles, technologie-gestütztes Comeback der sozialen Währungen sein, und sie könnten sogar weit über ihre Rolle im 19. und 20. Jahrhundert hinauswachsen und zu einer starke Mainstream-Kraft in der Weltwirtschaft werden.

Wie also wird es weitergehen? Dogecoin hat der Öffentlichkeit bereits gezeigt, wie leicht die Erschaffung einer eigenen Währung ist. Tatsächlich hat der Bitcoin-Entwickler Matt Corallo auch eine Site – coingen.io – erstellt, mit deren Hilfe User durch ein paar kleine Parameteränderungen schnell ihre eigenen Bitcoin- oder Litecoin-Klone erschaffen können. Ungeachtet der begrenzten Auswahl an Optionen, die die Site gegenwärtig hat, hat sie sich als recht populär erwiesen: Mithilfe dieses Service wurden trotz der Gebühr von 0,05 BTC Hunderte Coins erschaffen. Sobald Coingen es Usern erlaubt, auch das Proof-of-Excellence-Mining anzuwenden, ihnen die Option bietet, einen Teil der Emission einer bestimmten Organisation oder einem Fonds zukommen zu lassen, und weitere Optionen für ein maßgeschneidertes Branding anbietet, werden wir vielleicht erleben, dass Tausende von Kryptowährungen aktiv im Internet in Umlauf gebracht werden.

Werden Währungen ihr Versprechen einlösen? Also eine dezentralere und demokratischere Art des Poolens unseres Geldes und der Unterstützung öffentlicher Projekte und Aktivitäten, die uns der Gesellschaft, die wir uns wünschen, näher bringen? Vielleicht, aber vielleicht auch nicht. Jetzt jedoch, da fast jeden Tag eine neue Kryptowährung veröffentlicht wird, sind wir verlockend nahe daran, es herauszufinden.

ETHEREUM: EINE KRYPTOWÄHRUNG DER NÄCHSTEN GENERATION UND EINE DEZENTRALE ANWENDUNGSPLATTFORM

Bitcoin Magazine, 23. Januar 2014

Im Lauf des letzten Jahres wurde zunehmend über sogenannte Bitcoin-2.0-Protokolle diskutiert – alternative kryptografische Netzwerke, die von Bitcoin inspiriert wurden, aber die zugrunde liegende Technologie für Zwecke weit über Währungen hinaus nutzbar machen wollen. Die früheste Implementierung dieser Idee war Namecoin, eine Bitcoin-ähnliche Währung aus dem Jahr 2010, die für die dezentrale Registrierung von Domain-Namen genutzt wurde. Seit Neuestem erleben wir das Aufkommen von Colored Coins, die es Usern erlauben, im Bitcoin-Netzwerk ihre eigenen Währungen zu erschaffen, sowie fortgeschrittener Protokolle wie Mastercoin, BitShares und Counterparty, die Leistungen wie Finanzderivate, Spar-Wallets und dezentrale Börsentransaktionen anbieten.

Allerdings waren alle bisher erfundenen Protokolle spezialisiert, das heißt, sie bemühten sich, detaillierte Feature-Sets für spezifische Wirtschaftszweige beziehungsweise – in der Regel finanzielle – Anwendungen maßzuschneidern. Jetzt aber schlägt eine Gruppe von Entwickler:innen, zu denen auch ich gehöre, ein Projekt mit umgekehrter Herangehensweise vor: ein Kryptowährungsnetzwerk, das so generalisiert wie möglich sein und allen Usern erlauben soll, darauf aufbauend spezielle Anwendungen für alle erdenklichen Zwecke zu entwickeln. Das Projekt: Ethereum.

Kryptowährungsprotokolle sind wie Zwiebeln …

Eine verbreitete Designphilosophie vieler 2.0-Protokolle von Kryptowährungen ist die Auffassung, dass Kryptowährungen, wie das Internet, am besten so designt werden sollten, dass sich ihre Protokolle in verschiedene Layers (Schichten) aufspalten. Gemäß dieser Auffassung sollte man sich Bitcoin als eine Art TCP/IP(Transmission Control Protocol/Internet Protocol)-Netzwerkprotokoll des Kryptowährungsökosystems vorstellen, auf dessen Grundlage andere Protokolle der nächsten Generation erstellt werden können, ganz ähnlich wie SMTP für E-Mail, http für Webseiten und XMPP für Chats – alle aufbauend auf TCP als einer gemeinsamen zugrunde liegenden Datenschicht.

Bislang sind Colored Coins, Mastercoin und Counterparty die drei wichtigsten Protokolle, die sich an diesem Modell orientiert haben. Die Funktionsweise des Colored-Coins-Protokolls ist einfach: Um Colored Coins zu erschaffen, markieren User zunächst einmal spezifische Bitcoins mit einer besonderen Bedeutung – wenn Bob zum Beispiel ein Goldemittent ist, möchte er vielleicht einen Satz Bitcoins »taggen« (auszeichnen), und er sagt, dass jeder Satoshi 0,1 Gramm Gold repräsentiert und bei ihm eingelöst werden kann. Das Protokoll spürt dann diese Bitcoins in der Blockchain auf, was es möglich macht, jederzeit die Besitzer:innen zu berechnen.

Mastercoin und Counterparty sind etwas abstrakter, denn sie nutzen die Bitcoin-Blockchain für die Datenspeicherung. Eine Mastercoin- oder Counterparty-Transaktion ist also eine Bitcoin-Transaktion, aber die Protokolle interpretieren diese auf ganz unterschiedliche Weise. Man kann zwei Mastercoin-Transaktionen haben, bei denen einmal 1 MSC und einmal 100 000 MSC gesendet werden, aber aus der Sicht der Bitcoin-User, die nicht wissen, wie dieses Mastercoin-Protokoll funktioniert, sehen beide aus wie kleine Transaktionen, bei denen jeweils 0,0006 BTC versendet wurden. Die Mastercoin-spezifischen Metadaten sind in den Transaktionsergebnissen encodiert. Anschließend muss ein Mastercoin-Client die Bitcoin-Blockchain nach Mastercoin-Transaktionen durchsuchen, um die aktuelle Bilanz zu ermitteln.

Ich hatte das Privileg, mich direkt mit vielen der Erfinder:innen des Colored-Coins- und Mastercoin-Protokolls unterhalten zu können, und war in erheblichem Maße an der Entwicklung beider Projekte beteiligt. Im Verlauf der rund zweimonatigen intensiven Mitarbeit wurde mir jedoch schließlich bewusst, dass die zugrunde liegende Idee, solche höheren Protokolle auf tieferschichtigen Protokollen aufzubauen, zwar lobenswert sei, die gegenwärtigen Implementierungen jedoch grundlegende Mängel aufwiesen, die wohl verhindern würden, dass die Projekte jemals mehr als nur eine geringe Resonanz finden werden.

Das liegt nicht daran, dass die den Protokollen zugrunde liegenden Ideen selbst schlecht wären. Mitnichten, denn die Ideen sind hervorragend und allein die Reaktion der Community beweist hinlänglich, dass sie sich um etwas dringend Benötigtes bemühen. Vielmehr liegt es daran, dass das tiefschichtige Protokoll, auf dem sie ihre höheren Protokolle aufsetzen wollen – also Bitcoin –, für die Aufgabe schlicht ungeeignet ist. Dies soll nicht heißen, dass Bitcoin schlecht oder keine revolutionäre Erfindung wäre; als Protokoll für die Wertspeicherung und -übertragung ist sie hervorragend. Allerdings ist sie für ein effektives tiefschichtiges Protokoll zu wenig leistungsfähig; Bitcoin gleicht weniger einem TCP, auf dem man HTTP aufbauen kann, sondern mehr einem SMTP: ein Protokoll, das die ihm zugedachten Aufgaben gut erledigt (im Fall von SMTP E-Mail, im Fall von Bitcoin Geld[-schöpfung]), sich daher aber nicht besonders gut als Grundlage von allem anderen eignet.

Bitcoin hat jedoch eine große Schwachstelle: Skalierbarkeit. Bitcoin selbst ist so skalierbar, wie es eine Kryptowährung nur sein kann; selbst wenn die Größe der Blockchain auf über ein Terabyte in die Höhe schießen sollte, gibt es ein im *Bitcoin-Whitepaper* beschriebenes, als »vereinfachte Zahlungsverifizierung« (SPV) bezeichnetes Protokoll, das »Light Clients« mit nur ein paar Megabytes Bandbreite und Speicherplatz erlaubt, sicher herauszufinden, ob sie Transaktionen empfangen haben oder nicht. Mit Colored Coins und Mastercoin verschwindet diese Möglichkeit jedoch. Aus folgendem Grund: Um herauszufinden, welche Farbe ein Colored Coin hat, muss man nicht nur die vereinfachte Zahlungsverifizierung von Bitcoin nutzen, um dessen Existenz zu beweisen, sondern man muss ihn auch bis zu seinem Ursprung zurückverfolgen und unterwegs bei jedem Schritt eine

SPV-Überprüfung durchführen. Manchmal muss der rückwärtsgerichtete Scan eine exponenziell wachsende Anzahl Transaktionen prüfen, und bei Metacoin-Protokollen muss man sogar jede einzelne Transaktion prüfen, um etwas herauszufinden.

Genau das will Ethereum korrigieren. Es will kein Protokoll im Stil eines Schweizer Armeemessers sein, mit Hunderten von Features für jedes Bedürfnis. Vielmehr strebt Ethereum danach, ein überlegenes Basisprotokoll zu sein, auf dem – als Alternative zu Bitcoin – andere dezentrale Anwendungen aufbauen können. Es bietet mehr Tools an, mit denen gearbeitet werden kann, und verschafft sämtliche Vorteile der Skalierbarkeit und Effizienz von Ethereum.

Kontrakte, nicht nur über Differenzen

Als Ethereum gerade entwickelt wurde, bestand ein großes Interesse an der Zulassung von Finanzkontrakten auf Basis von Kryptowährungen – der Grundtyp dessen ist ein »Differenzkontrakt« (CFD). Bei einem solchen erklären sich zwei Parteien zur Investition eines gewissen Geldbetrags bereit und sie erhalten einen Erlös, dessen Höhe proportional zu dem Wert eines zugrunde liegenden Vermögenswertes ist. So könnte zum Beispiel Alice bei einem CFD 1000 Dollar investieren, während Bob ebenfalls 1000 Dollar einsetzt. Nach 30 Tagen würde die Blockchain dann automatisch an Alice 1000 Dollar plus 100 Dollar für jeden Dollar, um den der LTC(Lightcoin)/USD-Kurs in diesem Zeitraum gestiegen ist, auszahlen, während Bob den Rest erhalten würde. Diese Kontrakte ermöglichen es, ohne zentrale Börse mit großer Hebelwirkung auf Vermögenswerte zu spekulieren beziehungsweise sich gegen die Schwankungsanfälligkeit von Kryptowährungen abzusichern, indem man ihr Wertänderungsrisiko ausschaltet.

Jetzt ist allerdings klar, dass Differenzkontrakte ein Sonderfall eines allgemeineren Konzepts sind: Formelkontrakte. Statt eines Kontrakts, der x Dollar von Alice und y Dollar von Bob einnimmt und x Dollar plus zusätzlicher z Dollar für jeden Dollar, um den ein bestimmter Kurs steigt, auszahlt, sollte ein Kontrakt Alice einen Kapitalbetrag zurückzahlen kön-

nen, der sich nach einer mathematischen Formel berechnet – dies würde Kontrakte beliebiger Komplexität erlauben. Wenn die Formel Zufallsdaten als Eingaben zulässt, können diese verallgemeinerten CFDs sogar zur Implementierung einer Art Peer-to-Peer-Glücksspiel genutzt werden.

Ethereum greift diese Idee auf und geht weiter: Statt Vereinbarungen zwischen zwei Parteien zu sein, die einen Anfang und ein Ende haben, sind Kontrakte in Ethereum eine Art autonomer Agent, der von der Blockchain simuliert wird. Jeder Ethereum-Kontrakt hat seinen eigenen Skriptcode, und dieser wird jedes Mal bei einer an ihn gesendeten Transaktion aktiviert. Die Skriptsprache hat Zugriff auf den Transaktionswert, den Absender und optionale Datenfelder sowie auf einige Blockdaten und ihren eigenen internen Speicher als Eingaben. Zudem kann sie Transaktionen senden. Um einen CFD zu erstellen, würde Alice einen Kontrakt erstellen und ihn mit einer Kryptowährung im Wert von 1000 Dollar unterlegen. Dann würde sie warten, bis Bob den Kontrakt annimmt, indem er ebenfalls 1000 Dollar senden würde. Der Kontrakt würde so programmiert, dass er einen Zeitmesser starten würde, sodass Alice oder Bob nach 30 Tagen eine kleine Transaktion an den Kontrakt senden könnten, um die Gelder freizugeben.

Code-Beispiel eines Ethereum-Währungskontrakts, geschrieben in einer höherschichtigen Sprache:

```
if tx.value < 100 * block.basefee:
stop
if contract.memory[1000]:
from = tx.sender
to = tx.data[0]
value = tx.data[1]
if to <= 1000:
stop
if contract.memory[from] < value:
stop
contract.memory[from] = contract.memory[from] - value
contract.memory[to] = contract.memory[to] + value
else: contract.memory[mycreator] = 10000000000000000
contract.memory[1000] = 1
```